

UNITED STATES DISTRICT COURT

for the
District of South DakotaIn the Matter of the Seizure and Search of:)
The content of one cellular phone belonging to)
Travis John McDonald and currently in the)
custody of ICAC)
)
)Case No. 20-174

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

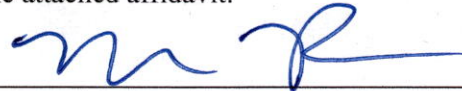
- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2422(b)Offense Description
Enticement of a Minor Using the Internet

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.



Special Agent Michelle Pohlen, HSI

*Printed name and title*Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.Date: 8-12-20*Judge's signature*City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate

Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEIZURE
AND SEARCH OF:

The content of one cellular phone
belonging to Travis John McDonald and
currently in the custody of ICAC

CASE NUMBER: 20-174

**AFFIDAVIT IN SUPPORT OF
SEARCH WARRANT
APPLICATION**

State of South Dakota)
) ss
County of Pennington)

I, Michelle Pohlen, Special Agent with Homeland Security Investigations (HSI), and currently assigned to the Rapid City, South Dakota Resident Agent in Charge (RAC) Office, being duly sworn, states as follows:

1. I have been a Special Agent (SA) with HSI since March 2019. In 2019, I completed the Homeland Security Investigations Special Agent Training (HSISAT) and Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. Since then, I have received specialized training in advanced child exploitation investigations and advanced victim identification. I have been working with the South Dakota Internet Crimes Against Children (ICAC) Task Force since October 2019. Prior to becoming a Special Agent, I was employed as a Federal Air Marshal with the Federal Air Marshal Service (FAMS) for two and a half years. Prior to FAMS, I served as a Police Officer with the Savannah Chatham Metropolitan Police Department (SCMPD) in Savannah, Georgia for one and a half years. I received a Bachelor of Arts degree in Law Enforcement in 2014.

2. During my law enforcement career I have become familiar with the *modus operandi* of persons involved in attempted commercial sex trafficking of a minor, in violation of federal law. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally attempt to meet with children in order to engage in criminal sex acts.

3. The information set forth below is based upon my knowledge of an investigation conducted by the South Dakota Internet Crimes Against Children Taskforce (ICAC) and the investigation of other law enforcement agents and officers including, but not limited to, South Dakota Division of Criminal Investigation (DCI), Homeland Security Investigations (HSI), the Rapid City Police Department, and the Pennington County Sheriff's Office. I have not included every fact obtained pursuant to this investigation, but have set forth those facts that I believe are essential to establish the necessary probable cause for the criminal complaint. I have not omitted any material fact relevant to the consideration of probable cause for a criminal complaint against the above named defendant.

4. I have been informed that 18 U.S.C. § 2422(b) makes it a crime for a person to knowingly attempt to engage in an unlawful sex act with a person who has not attained the age of 18. Your affiant respectfully submits that there is probable cause to believe that Travis John McDonald committed the crime of attempted enticement of a minor using the internet in violation of 18 U.S.C. § 2422(b) and utilized the SUBJECT DEVICE to commit the crime.

ITEMS TO BE SEARCHED FOR AND SEIZED:

5. The undersigned respectfully requests that a search warrant be issued to permit a search of the content of one cellular phone, belonging to Travis John McDonald seized from his vehicle upon his August 10, 2020 arrest. Further described as one Black iPhone in off-white clear case with Copenhagen sticker and several other stickers and ICCID 89014104272048066109.

6. The warrant is sought in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b), enticement of a minor using the internet.

DEFINITIONS

7. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Chat*: as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. *Child Erotica*: as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. *Child pornography*: as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. *Cloud-based storage service*: as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. *Computer*: The term “computer” means “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data

storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet.

f. *Computer Hardware:* The term “computer hardware” means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. *Computer-related documentation:* as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. *Computer Passwords and Data Security Devices:* The term

“computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. *Computer-Related Documentation:* The term “computer-related documentation” means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. *Computer Software:* The term “computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

k. *Electronic Communication Service (“ESP”):* as defined in 18 U.S.C. § 2510(15), is a provider of any service that gives to users thereof

the ability to send or receive wire or electronic communications. For example, “telephone companies and electronic mail companies” generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

l. *Electronic Storage Device*: includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any “cloud” storage by any provider.

m. *File Transfer Protocol* (“FTP”): as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

n. *Internet*: The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. *Internet Connection*: The term “Internet connection” means a connection required for access to the Internet. The connection would

generally be provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

p. *Minor*: The term “minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

q. *Records, documents, and materials*: as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

r. *Remote Computing Service (“RCS”)*: as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

s. *Short Message Service (“SMS”)*: as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

t. *Storage Medium*: The term “storage medium” refers to any physical object upon which computer data can be recorded. Examples

include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

u. *Visual Depictions*: “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

v. *Wireless Network*: The term “wireless network” means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer, which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. However, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

PROBABLE CAUSE

8. On August 10, 2020, HSI SA Lawrence Propes was posing as a 13-year-old female in an online operation targeting predators. He was on the

internet application MeetMe, which operates solely online. At 4:52p.m., a person later identified as 28 year old Travis John McDonald, began communicating with Propes' UC profile. He asked if "she" was interested in "FWB" (which I know means friends who have sex). Propes advised McDonald that he was "younger" and McDonald responded that younger means "tighter and more fun." Propes and McDonald began to communicate via text message and Propes informed McDonald he was only 13 years old. After that, McDonald continued his sexually driven conversation with the undercover minor including writing, "oral, then go from there and if you want I will fuck you." He also agreed to wear condoms. He said, "Want to meet up and get your pussy ate out." He also asked "how many fingers can you fit into your pussy," on at least two occasions.

9. McDonald sent two images of his semi-flaccid penis. During the conversation, McDonald sought to meet the minor to engage in the above acts. The meeting was set at a location in Rapid City, South Dakota. McDonald appeared at the previously determined location and time and law enforcement placed him under arrest. The SUBJECT DEVICE was seized from McDonald's vehicle and placed in evidence.

10. McDonald was later interviewed and admitted it was he chatting, admitted to sending specific messages and sending the lewd photos. He acknowledged that the minor told him she was only 13.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS INCLUDING CELL PHONES

11. Based upon my training and experience, as well as information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during a search of physical premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to

conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

12. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give the target an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

LIMIT ON SCOPE OF SEARCH

13. I submit that if during the search, agents find evidence of crimes not set forth in this affidavit, another agent or I will seek a separate warrant.

CONCLUSION

14. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, is located on the SUBJECT DEVICE, described further in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT DEVICE, authorizing the seizure and search of the items described in Attachment B.

15. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar

process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



MICHELLE POHLEN
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN to

de in my presence
by reliable electronic means

this 12th day of August, 2020.



DANETA WOLLMANN
U.S. MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Seized and Searched

One cellular phone, belonging to Travis John McDonald seized from his vehicle upon his August 10, 2020 arrest. Further described as one black in color iPhone in off-white clear case with Copenhagen sticker and several other stickers and ICCID 89014104272048066109.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of 18 U.S.C. § 2422(b), enticement or attempted enticement of a minor using the internet:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERS"):
 - a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERS;
 - h. evidence of the times the COMPUTERS were used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTERS;

- j. documentation and manuals that may be necessary to access the COMPUTERS or to conduct forensic examinations of the COMPUTERS;
 - k. records of or information about Internet Protocol addresses used by the COMPUTERS;
 - l. records of or information about the COMPUTERS' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
 - 4. Child pornography and child erotica.
 - 5. Records, information, and items relating to violations of the statutes described above including
 - a. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
 - b. Records and information relating to sexual exploitation of children, including correspondence and communications between Whisper app users.
 - 6. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
 - 7. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones (cell phones), tablets, certain gaming devices, server computers, and network hardware.
 - 8. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include but are not limited to internal and external hard drives, SD cards, storage disks (CDs and DVDs), flash memory, other magnetic or optical media and "cloud" storage by any provider.

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Seizure and Search of:

The content of one cellular phone belonging to)
Travis John McDonald and currently in the)
custody of ICAC)

Case No. 20-174

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. § 2422(b) as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before Aug 26, 2020 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 8-12-20 10:45am

City and state: Rapid City, SD



Judge's signature

Daneta Wollmann, U.S. Magistrate

Printed name and title

cc: AUSA Collins
JAR

[illegible]